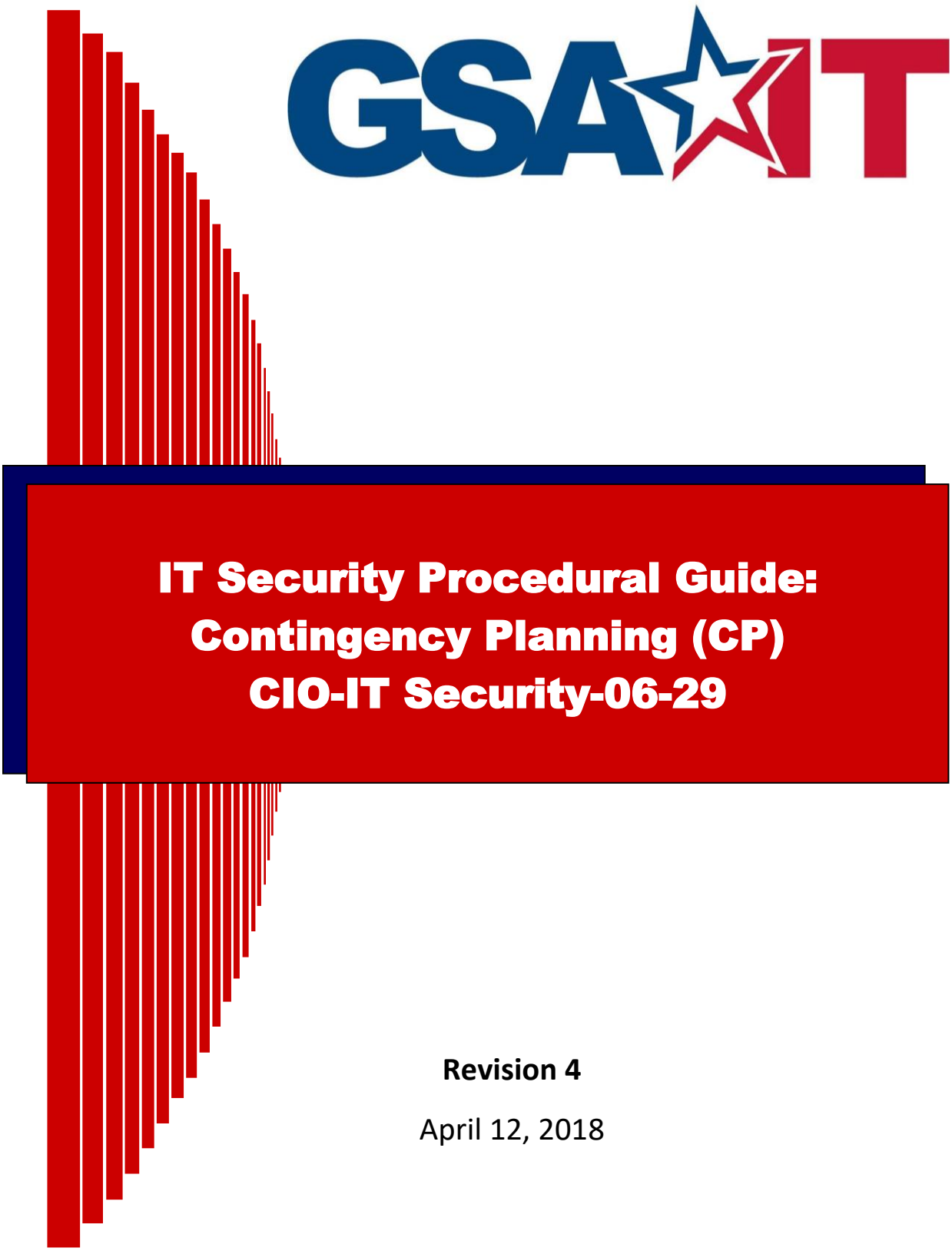

IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29

Revision 4

April 12, 2018

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 Changes – February 22, 2007				
1	Bo Berlas	Clarified functional testing requirement.	NIST 800-53, R1.	6
2	Bo Berlas	New Appendix E	OIG Audit recommendation for agency guidance for contingency plan training, plan maintenance, and backups.	22
Revision 2 Changes – August 16, 2010				
1	Berlas/ Cook	Updated NIST controls to align with SP 800-53 Revision 3.	NIST 800-53, R3.	Throughout
Revision 3 Changes – March 9, 2016				
1	Sitcharing/ Wilson	Updated NIST controls to align with SP 800-53 Revision 4.	NIST 800-53, R4 &IT Security Program Plan	Throughout
Revision 4 Changes - April 12, 2018				
1	Feliksa/ Dean	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework.	Biennial update.	Throughout

APPROVAL

IT Security Procedural Guide: Contingency Planning (CP), CIO-IT Security-06-29, Revision 4 is hereby approved for distribution.

4/12/2018

X Kurt Garbars

Kurt Garbars
GSA Chief Information Security Officer
Signed by: KURT GARBARS

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

Table of Figures and Tables

1 Introduction

Contingency planning focuses on the recovery and restoration of an Information Technology (IT) system following a disruption. General Services Administration (GSA) Order OMA 2430.2, "*The U.S. General Services Administration Continuity of Operations Mission Essential Functions*" supports the agency Continuity of Operations Plan (COOP) required by Presidential Policy Directive (PPD) 40, "*National Continuity Policy*" ensuring that primary mission-essential functions continue to be performed during a wide range of emergencies. Contingency and continuity of support plans must be developed and tested for all IT systems in accordance with Office of Management and Budget (OMB) Circular No. A-130, "*Managing Information as a Strategic Resource,*" National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*," and GSA policies, directives, and procedures.

Every GSA IT system must follow the Contingency Planning (CP) practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,*" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and approved by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

The CP principles and practices described in this guide are based on guidance from NIST including NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations."* This guide provides an overview of CP, roles and responsibilities, NIST SP 800-53 CP requirements per Federal Information Processing Standards (FIPS) Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems*," security categorization level, and procedures for implementing these requirements.

Executive Order (EO) 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"* requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*" Table 1-1, NIST SP 800-53 Control to CSF Mapping, provides how the NIST SP 800-53 controls

within this guide are aligned with the CSF Category Unique Identifiers. The following CSF categories are aligned with NIST's CP controls.

- Identify-Governance (ID.GV)
- Identify-Asset Management (ID.AM)
- Identify-Business Environment (ID.BE)
- Identify-Supply Chain Risk Management (ID.SC)
- Protect-Data Security (PR.DS)
- Protect-Information Protection Processes and Procedures (PR.IP)
- Protect-Protective Technology (PR.PT)
- Detect-Anomalies and Events (DE.AE)
- Respond-Response Planning (RS.RP)
- Respond-Communications (RS.CO)
- Respond-Analysis (RS.AN)
- Respond-Improvements (RS.IM)
- Recover-Communications (RC.CO)
- Recover-Recovery Planning (RC.RP)

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Controls	CSF Category Unique Identifier Codes
CP-1	ID.GV-1, ID.GV-3
CP-2	ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-9, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3
CP-3	RS.CO-1
CP-4	ID.SC-5, PR.IP-4, PR.IP-10
CP-6	PR.IP-4
CP-7	PR.IP-9, PR.PT-5
CP-8	ID.BE-4, PR.PT-4, PR.PT-5
CP-9	PR.IP-4
CP-10	RS.RP-1, RC.RP-1

1.1 Purpose

The purpose of this guide is to provide guidance for the CP security controls identified in NIST SP 800-53 and contingency planning requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in the contingency planning of IT assets the specific procedures and processes they are to follow for GSA information systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the contingency planning of GSA information systems and data.

1.3 Policy

Chapter 4, paragraph 2 of CIO 2100.1 states:

d. IT contingency planning/continuity of support planning.
Contingency planning focuses on the recovery and restoration of an IT system following a disruption. The contingency plan supports the agency Continuity of Operations Plan (COOP) required by PPD-40, National Continuity Policy, ensuring that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies. Contingency and continuity of support plans must be developed and tested annually for all IT systems IAW OMB Circular No. A-130, NIST SP 800-34, and GSA CIO-IT Security-06-29.

(1) A system specific IT contingency plan must be developed that identifies and addresses preventive controls, damage assessment procedures, plan testing and training procedures.
(2) Each contingency plan must include an approved BIA recovery strategy and documented procedures to maintain the plan.
(3) Personnel supporting FIPS 199 Low, Moderate and High impact systems with contingency planning responsibilities shall be trained in their contingency roles and responsibilities with respect to the information system annually with refresher training every three years.
(4) The contingency plan must be annually tested IAW GSA CIO-IT Security-06-29.
(5) COOP contact lists which only contain a person's name and home phone number are exempt from GSA IT security policy requirements in this policy. COOP contact lists kept on an electronic device that is password protected (other Government approved Smart Phone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists" limited to name and home phone number that are maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media should be kept in a locked facility or an otherwise secure location when not in use.
(6) *The contingency plan must be updated annually to address system/organizational changes or problems encountered during plan implementation, execution, or testing.*

1.4 References

Federal Standards, Regulations, and Publications:

- EO 13800, *"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*
- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- NIST Cybersecurity Framework, *"Framework for Improving Critical Infrastructure Cybersecurity"*
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"

- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"*
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-84, "*Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities*"
- NIST SP 800-161, "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*"
- OMB Circular No. A-130, "*Managing Information as a Strategic Resource*"

GSA Policies and Procedures:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2140.4, "*GSA Information Technology (IT) Solutions Life Cycle (SLC) Policy*"
- GSA Order OMA 2430.2, "*The U.S. General Services Administration Continuity of Operations Mission Essential Functions*"
- CIO-IT Security-01-02, *"Incident Response (IR)"*
- CIO-IT Security-18-90, "*Information Security Program Plan*"

2 Contingency Planning Roles and Responsibilities

There are many roles associated with implementing effective contingency planning for IT systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide, specific processes and procedures for implementing NIST's CP controls are described.

2.1 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring Information Assurance is included in management planning, programming budgets, and the IT Capital Planning process.
- Ensuring contingency and continuity of support plans are developed, maintained, and tested annually.

2.2 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Ensuring assessment and authorization support documentation, including contingency plans and test reports, are developed and maintained.
- Reviewing and coordinating reporting of Security Advisory Alerts, compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.

2.3 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Assisting in the development and maintenance of contingency plan and contingency plan test report documentation.
- Assisting in the identification, implementation, and assessment of a system's security controls, including common controls.
- Working with the ISSM and system owners to develop, implement, and manage Plans of Action and Milestones (POA&Ms).

2.4 System Owners (e.g., System Program Managers/Project Managers)

Responsibilities include the following:

- Participating in activities related to the assessment and authorization of the system to include security planning, risk assessments, security and incident response testing, and contingency planning and testing.
- Developing, implementing and maintaining an approved IT Contingency Plan which includes an acceptable Business Impact Analysis (BIA).
- Coordinating with IT security personnel including the ISSM and ISSO and Data Owners to ensure implementation of system and data security requirements
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms.

2.5 Data Owners

Responsibilities include the following:

- Coordinating with system owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected in accordance with GSA policies, regulations and guidelines.
- Coordinating with IT security personnel including the ISSM and ISSO and system owners to ensure implementation of system and data security requirements.

2.6 Custodians

Responsibilities include the following:

- Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.
- Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.

2.7 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Implementing system backups and patching of security vulnerabilities.
- Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented.

3 IT Contingency Planning Process

Contingency planning is a coordinated strategy involving plans, procedures, and technical measures that enable a system to be recovered as quickly and effectively as possible following a service disruption. The process is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and its FIPS 199 security categorization level.

Contingency planning generally includes one or more of the following approaches to restore disrupted services:

- Restoring information systems using alternate equipment;
- Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
- Recovering information systems operations at an alternate location (typically acceptable for only long-term disruptions or those physically impacting the facility); and
- Implementing appropriate NIST SP 800-53 contingency planning controls based on the information system's FIPS 199 security impact level.

NIST SP 800-34 details a seven-step methodology for developing an IT contingency process and plan. Planning, implementing, and testing the contingency strategy are addressed by six of the seven steps; documenting the plan and establishing procedures and personnel organization to implement the strategy is the final step. The steps are common to all information systems. Figure 3-1 (also Figure 3-1 in NIST SP 800-34) illustrates the key elements in the contingency planning process.

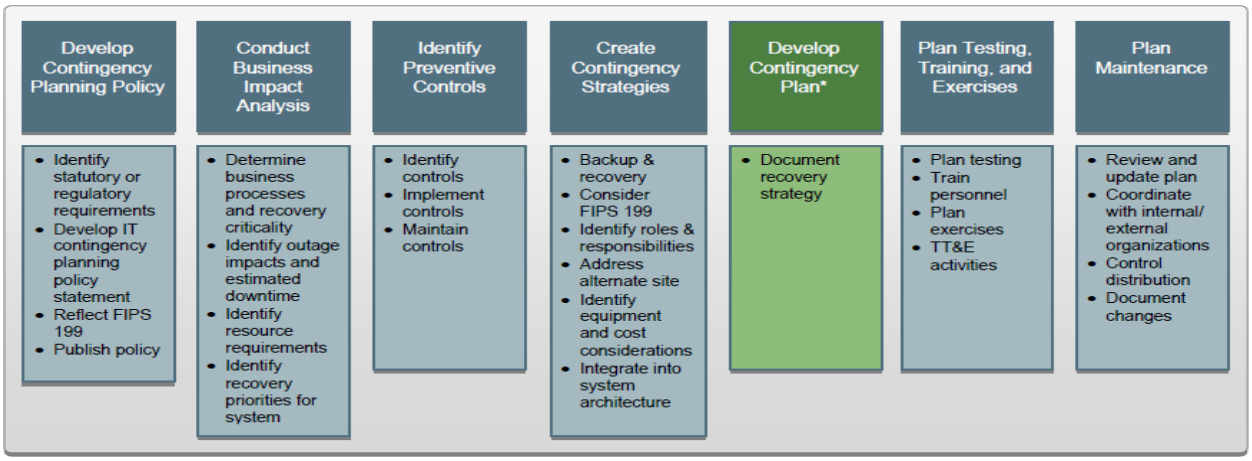

Figure 3-1: Contingency Planning Process

All information systems must have well developed and tested contingency plans in place to facilitate the recovery of systems, data and operations after a disruption. The following sections detail the steps in the contingency planning process.

3.1 Step 1 – Develop the Contingency Planning Policy Statement

The first step in the process is to develop the contingency planning policy statement. This is critical to ensure personnel fully understand GSA's contingency planning requirements as stated in CIO Order 2100.1 and this guide.

As documented in NIST SP 800-34, the following key elements are reflected in the GSA contingency planning policy statement:

- Roles and responsibilities;
- Scope as applies to common platform types and organization functions (i.e., telecommunications, legal, media relations) subject to contingency planning;
- Resource requirements;
- Training requirements;
- Exercise and testing schedules;
- Plan maintenance schedule; and
- Minimum frequency of backups and storage of backup media.

3.2 Step 2 – Conduct the Business Impact Analysis

Completion of the BIA is one of the key steps in implementing the CP controls in NIST SP 800-53, and in the contingency planning process overall. It enables GSA associates and contractors with contingency planning responsibilities to characterize the system components, supported mission/business functions, and interdependencies. The BIA correlates the system with the critical mission/business processes and services provided, and based on that information, characterizes the consequences of a disruption.

The BIA should be started during the Initiation phase of the GSA Solutions Lifecycle (SLC) in accordance with GSA Order CIO 2140.4, "*GSA Information Technology (IT) Solutions Life Cycle (SLC) Policy.*" As the system design evolves and components change, the BIA may need to be updated during the Planning and Execution phases of the SLC. All information systems are required to conduct a BIA as part of the overall contingency planning process. The BIA development process as detailed by NIST SP 800-34, typically consists of the following steps:

- Determine mission/business functions and recovery criticality.
- Identify resource requirements.
- Identify recovery priorities for system resources.

Results of the BIA are used to determine any system specific contingency planning requirements and priorities and can be incorporated into the analysis and strategy development efforts for the COOP, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). The BIA process is fully detailed in NIST SP 800-34. A BIA template can be found on the GSA IT Security Forms InSite webpage.

3.3 Step 3 – Identify Preventive Controls

Outage impacts to the information system that have been identified in the BIA can be mitigated through the implementation of preventive controls. Preventive controls are technical measures or operational procedures taken to deter, reduce, and/or detect impacts to the information system and to prevent system disruption. Where feasible and cost-effective, preventive methods are recommended over any actions necessary to recover the system. Preventive controls are identified in NIST SP 800-53. Depending on the system type and its configuration, common measures may include such things as:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls);
- Gasoline-or diesel-powered generators to provide long-term backup power;
- Air-conditioning systems with adequate excess capacity to prevent failure of certain components, such as a compressor;
- Fire suppression systems;
- Fire and smoke detectors;
- Water sensors in the computer room ceiling and floor;
- Heat-resistant and waterproof containers for backup media and vital non electronic records;
- Emergency master system shutdown switch;
- Offsite storage of backup media, non-electronic records, and system documentation;
- Technical security controls, such as cryptographic key management; and
- Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage.

3.4 Step 4 – Create Contingency Strategies

Contingency strategies are used to mitigate risks associated with the contingency planning family of controls in NIST SP 800-53 and may vary depending on the FIPS 199 security impact level for the information system. As documented in NIST SP 800-34, these strategies generally cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance of the information system. Detailed backup and recovery guidance for implementing appropriate backup and recovery strategies to restore system operations following a disruption can be found in Section 3.4 of NIST SP 800-34.

3.5 Step 5 – Develop an Information System Contingency Plan

Development of the contingency plan is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption. The contingency plan documents the technical capabilities designed to support contingency operations. The contingency plan format must follow NIST SP 800-34. Contingency Plan Templates for FIPS 199 Low, Moderate, and High impact systems are available on the GSA IT Security Forms InSite webpage. The templates may be modified to accommodate system specific, operational, and/or organization requirements.

Figure 3-2 (Figure 4-1 in NIST SP 800-34) 4) identifies the five main components of the Contingency Plan. The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that must be taken following a system disruption or emergency. Detailed contingency plan development guidance can be found in Section 4 of NIST SP 800-34.

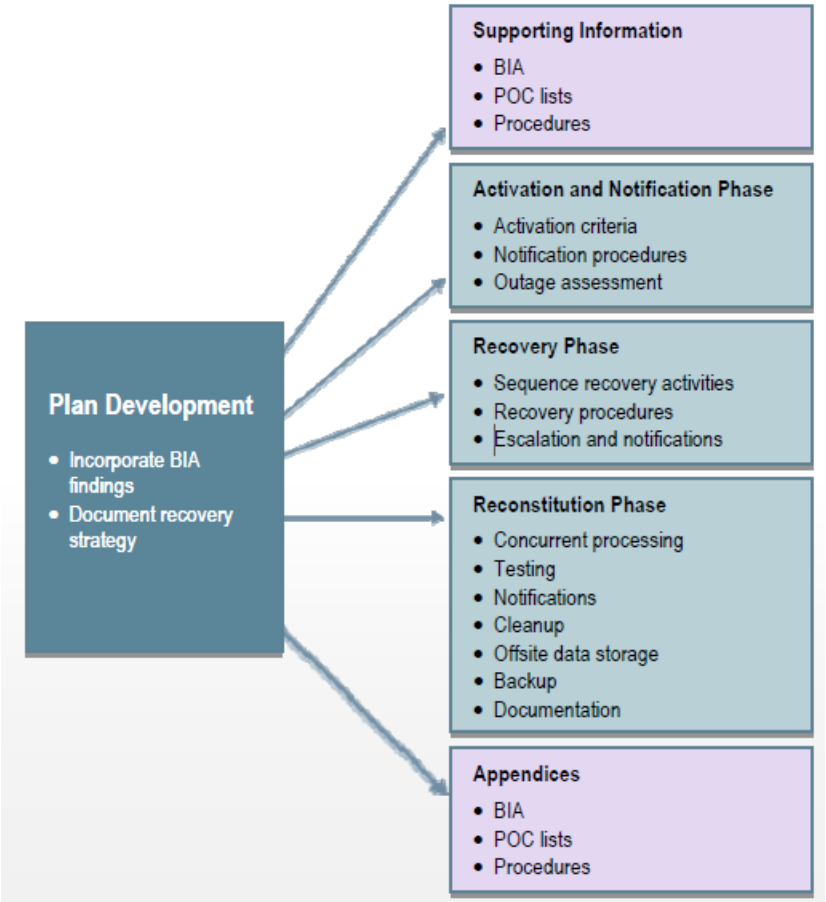

Figure 3-2: Contingency Plan Structure

3.6 Step 6 – Ensure Plan Testing and Exercises

The contingency plan must be maintained routinely and exercised/tested at least annually to continually refine resumption and recovery procedures to reduce the potential for failure. Contingency plan tests aid in determining the plan's overall effectiveness by enabling plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. The scope, scenario, and objective of each test should be varied to ensure that all of the elements of the contingency plan remain current and effective. NIST SP 800-84 provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events to capabilities to prepare for, respond to, manage, and recover from adverse events. Results from testing activities shall be documented in a Contingency Plan Test Report using the template available on the GSA IT Security Forms InSite webpage.

There are two categories of testing: *announced* and *unannounced*. In an announced test, personnel are instructed when testing will occur, what the objectives of the test are, and what the scenario will be for the test. Announced testing provides test participants the opportunity to prepare for the test in advance by becoming familiar with the procedures. Unannounced

testing involves testing without prior notification. Unannounced testing focuses on the adequacy of in-place procedures and team preparedness. The combination of both test types improves the accuracy of recovery procedures and the readiness of test participants. Regardless of the test type selected, all Contingency Plan Tests should address the following key areas (as applicable):

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations; and
- Other plan testing (where coordination is identified, i.e., COOP, BCP).

There are two basic formats for contingency plan tests, including:

- **Classroom or Tabletop Exercise:** Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.
- **Functional Exercises:** Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

The selection of a contingency plan test format will depend on the frequency of testing, cost, and time. GSA requires annual contingency plan testing for all systems to determine the plan's effectiveness and the organization's readiness to execute the plan. The depth and rigor of contingency plan testing activities increases with the FIPS 199 availability security objective. All tests and exercises should include some kind of determination of the effects on the organization's operations and provide for a mechanism to update and improve the plan as a result.

- **For low impact systems, an annual tabletop exercise is sufficient.** The tabletop should simulate a disruption, include all main contingency plan points of contact, and be conducted by the system owner or responsible authority;
- **For moderate impact systems, a functional exercise must be conducted at least once every three years. A tabletop exercise is acceptable in other years.** The functional

exercise is a simulation of a disruption to a system recovery component. The test should include all contingency plan points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media; and

- **For high impact systems, a functional exercise must be conducted annually.** The functional exercise is a simulation that may vary from a simulation of a disruption to system recovery component to a complete failure prompting a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state. The extent of the functional exercise is up to the GSA S/SO based on resources, previous exercises, and other system-specific factors.

3.6.1 Suggested Contingency Plan Test Actions/Key Processes

The following are suggested contingency plan test actions. These key processes are central to effective contingency plan testing and management. Steps 1-4 form the contingency test plan, step 5 is the exercise of the test plan, and step 6 involves revisions to the contingency plan and the contingency test plan following an exercise.

Step 1: Identify contingency plan elements to test: Review the contingency plan to select key procedures that must be tested and periodically revised to ensure that all of the elements of the contingency plan remain current and are effective. Refer to the Contingency Plan Logistics Checklist on the GSA IT Security Forms InSite webpage for aid in planning.

Step 2: Define test objectives: List the specific objective with success criteria for each test element and the overall test plan. Test objectives must include (as applicable):

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations; and
- Other plan testing (where coordination is identified, i.e., COOP, BCP).

Step 3: Identify test participants, pre-test information, location, schedule and environment: List each test participant and the specific roles they are to perform within the test, the test location, a test schedule, and affected system components (servers, workstation, and other components that will be tested).

Step 4: Define test scenario and test procedures: List the specific scenario that will be utilized for the test. In determining the scenarios consider both the worst-case incident and those incidents that are most likely to occur. Test scenarios should mimic reality as closely as possible. Appendix B contains a few sample test scenarios and expected outcomes. Document steps 1-4

in a contingency plan test plan. A Contingency Test Plan Template is available on the GSA IT Security Forms InSite webpage.

Step 5: Execute test and document results: Test results and lessons learned should be documented in a test report using the Contingency Plan Test Report Template. The results should be reviewed with the test participants and other personnel as appropriate.

Step 6: Revision of Contingency Plan: To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Periodic reviews of the plan must be conducted in addition to reviews whenever there are changes affecting:

- Operational requirements
- Security requirements
- Technical procedures
- Changes of hardware, software, and other equipment
- Changes with alternate facility requirements
- Changes with team members and team members contact information
- Changes with vendors and vendors contact information (including alternate and off-site vendor POCs)
- Vital records

3.7 Step 7 – Ensure Plan Maintenance

The contingency plan should be reviewed and updated annually to address system/organizational changes or problems encountered during plan implementation, execution, or testing. The contingency plan is a living document and must always be current. The plan must be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. At a minimum, plan reviews should focus on the following elements:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Hardware, software, and other equipment (types, specifications, and amount);
- Names and contact information of team members;
- Names and contact information of vendors, including alternate and offsite vendor POCs;
- Alternate and offsite facility requirements; and
- Vital records (electronic and hardcopy).

The plan reviews should also include review of supporting information to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

- Alternate site contract, including testing times;
- Offsite storage contract;

- Software licenses;
- Memorandums of Understanding (MOUs) or Service Level Agreements (SLAs);
- Hardware and software requirements;
- System interconnection agreements;
- Security requirements;
- Recovery strategy;
- Contingency policies;
- Training and awareness materials;
- Testing scope; and
- Other plans, e.g., COOP, BCP.

Although some changes may be quite visible, others will require additional analysis. When a significant change occurs, the BIA should be updated with the new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified. Finally, plan maintenance should be continued as the information system passes through the Disposal phase of its life cycle to ensure that the plan accurately reflects recovery priorities and concurrent processing changes.

Record changes to the plan on a change tracking matrix attached in the front of the document or in an appendix. The matrix should record the following information:

- Change number
- Person posting change
- Pages changed, deleted, or inserted
- Page comment
- Date change was posted
- Plan distribution

4 Implementation Guidance for CP Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements in this guide apply to GSA Federal employees and contractors who are involved in contingency planning of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section. If “None” is listed for “Additional Contractor System Considerations” it means there are no additional requirements, the system still needs to comply with the overall implementation guidance.

CP-1, Contingency Planning Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems by GSA and as a Hybrid Control for contractor systems. The CP-2 to CP-10, when included in a system’s control set, either are provided as a Common Control by a Major Information System, a system specific control by the system, or as a Hybrid

Control with shared responsibilities for control implementation. GSA's Information Security Program Plan (ISPP) describes the GSA enterprise-wide inheritable common and hybrid controls and outlines the responsible party for implementing each of them.

4.1 CP-1 Contingency Planning Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
    1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
    1. Contingency planning policy [*biennially*]; and
    2. Contingency planning procedures [*biennially*].

GSA Implementation Guidance: Control CP-1 is applicable at all FIPS 199 levels.

CP related Policies and Procedures are developed and then disseminated via the IT Security Procedural Guides InSite page and are reviewed/updated biennially.

CIO 2100.1 contains contingency planning policy for all GSA systems. As required, the policy addresses scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

CP procedures are documented throughout this guide. The procedures have been developed to facilitate the implementation of the contingency planning policy and associated NIST SP 800-53 controls.

Additional Contractor System Considerations:

Contractor systems may defer to GSA policy and procedures as identified above or separately implement policy and procedures that facilitate the implementation of the required contingency planning policies, procedures, and controls as per FIPS 199 impact level.

4.2 CP-2 Contingency Plan

Control: The organization:

a. Develops a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by [*the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), System Owner, and the Chief Information Security Officer (CISO)*];

b. Distributes copies of the contingency plan to [*the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), System Owner, and the Office of the Chief Information Security Officer (CISO)*];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system [*annually*];
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), System Owner, and the Chief Information Security Officer (CISO)*]; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Control Enhancements:

(1) Contingency Plan | Coordinate With Related Plans. The organization coordinates contingency plan development with organizational elements responsible for related plans.
(2) Contingency Plan | Capacity Planning. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
(3) Contingency Plan | Resume Essential Missions/Business Functions. The organization plans for the resumption of essential missions and business functions within [*a time period recommended by the GSA S/SO or Contractor in accordance with the Business Impact Analysis (BIA) and approved by the GSA AO*] of contingency plan activation.
(4) Contingency Plan | Resume All Missions/Business Functions. The organization plans for the resumption of all missions and business functions within [*a time period recommended by the GSA S/SO or Contractor in accordance with the Business Impact Analysis (BIA) and approved by the GSA AO*] of contingency plan activation.
(5) Contingency Plan | Continue Essential Missions/Business Functions. The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.
(8) Contingency Plan | Identify Critical Assets. The organization identifies critical information system assets supporting essential missions and business functions.

GSA Implementation Guidance: Control CP-2 is applicable at all FIPS 199 levels. Enhancements CP-2(1), (3), and (8) are applicable at the FIPS 199 Moderate and High levels. Enhancements CP-2(2), (4), and (5) are applicable at the FIPS 199 High level.

GSA 2100.1 requires all information systems to have a contingency plan in accordance with NIST SP 800-34 and this guide.

The contingency plan must be reviewed and tested annually and updated as-needed. This can be done either individually or in coordination with annual incident response plan testing or exercises as described in in Section 4.4 of CIO-IT Security-01-02, *"Incident Response (IR)."* Copies of the contingency plan must be distributed to personnel who have assigned incident response roles for the information system including the AO, ISSM, ISSO, PM, CISO, and ERC.

Information System Contingency Plan templates for each of the FIPS 199 impact levels are available on the GSA IT Security Forms InSite page.

For enhancements CP-2 (1), (3) and (8), FIPS 199 Moderate and High impact systems must coordinate their contingency plan testing/exercises with organizational elements responsible for related plans such as Disaster Recovery, Continuity of Operations (COOP) and/or Incident Response plans.

For enhancements CP-2 (2), (4), and (5), FIPS 199 High impact systems must plan for the recovery of the systems essential business functions and mission within the recovery timeframe established by the Business Impact Analysis. In addition, capacity planning must be performed in order to ensure that information processing, telecommunications and environmental support are matched to the needs of the information system, during contingency operations.

Additional Contractor System Considerations: *None.*

4.3 CP-3 Contingency Training

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [*30 days*] of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. [*Annually*] thereafter.

Control Enhancements:

(1) Contingency Training | Simulated Events. The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

GSA Implementation Guidance: Control CP-3 is applicable at all FIPS 199 levels. Enhancement CP-3(1) is applicable at the FIPS 199 High level.

All agency personnel with contingency planning responsibilities for any information system must be trained in their role(s) and responsibilities with respect to the information system. GSA requires contingency plan training to be conducted annually.

System specific contingency planning training should be integrated as part of GSA's major information systems' annual contingency plan test or integrated into COOP exercises.

Contingency training should complement testing activities to ensure personnel with contingency planning responsibilities are able to execute their respective recovery procedures without the aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. NIST SP 800-34 requires agency personnel with contingency planning responsibilities be provided training on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases) Individual responsibilities (Notification/Activation, Recovery, and Reconstitution Phases).

As stated in Chapter 2 of the NIST SP 800-84, training may consist of:

- Informing personnel of their role(s) and responsibilities
- Teaching them skills related to those role(s) and responsibilities

Training prepares personnel to perform the responsibilities when needed. Training should be structured to allow personnel to learn their responsibilities and demonstrate their understanding of them.

For enhancement CP-3(1), FIPS 199 High impact systems must incorporate simulated events into their contingency training, in order to ensure a more effective response in the event of system disruptions.

Additional Contractor System Considerations: *None.*

4.4 CP-4 Contingency Plan Testing

Control: The organization:

a. Tests the contingency plan for the information system [*annually*] using [*GSA IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Control Enhancements:

(1) Contingency Plan Testing | Coordinate With Related Plans. The organization coordinates contingency plan testing with organizational elements responsible for related plans.
(2) Contingency Plan Testing | Alternate Processing Site. The organization tests the contingency plan at the alternate processing site:
    (a) To familiarize contingency personnel with the facility and available resources; and
    (b) To evaluate the capabilities of the alternate processing site to support contingency operations.

GSA Implementation Guidance: Control CP-4 is applicable at all FIPS 199 levels. Enhancement CP-4(1) is applicable at the FIPS 199 Moderate and High levels. Enhancement CP-4(2) is applicable at the FIPS 199 High level.

Contingency plans for all information systems must be conducted annually in accordance with this guide and NIST SP 800-84. The activity can be implemented separately or integrated with the system's annual incident response plan test as described in Section 4.4 of CIO-IT Security-01-02, "Incident Response (IR)." If testing is integrated with a Major Information System's contingency plan testing both systems must document participation in the testing.

Annual testing validates the contingency plan's content as well as to improve the capabilities to prepare for, respond to, manage, and recover from adverse events that may affect GSA information systems. GSA contingency plan testing requirements per system impact level can be found in Section 3.6 of this guide, Step 6 – Ensure Plan Testing, Training, and Exercises.

Sample scenarios for testing activities can be found in (Appendix B) of this guide. Refer to NIST SP 800-84 for more specific guidance in developing, conducting, and evaluating contingency plan test activities. Results of the annual test should be documented using the contingency plan test report template available on the GSA IT Security Forms InSite page.

For enhancement CP-4(1), FIPS 199 Moderate and High impact systems must coordinate their contingency plan testing with organizational elements responsible for related plans such as Disaster Recovery, Continuity of Operations (COOP) and/or Incident Response plans.

For enhancement CP-4(2), FIPS 199 High impact systems must test the contingency plan at its alternate processing site to familiarize personnel with the alternate site and its resources and to gauge the alternate site's capabilities to perform system operations.

Additional Contractor System Considerations: *None.*

4.5 CP-6 Alternate Storage Site

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Control Enhancements:

(1) Alternate Storage Site | Separation from Primary Site. The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
(2) Alternate Storage Site | Recovery Time / Point Objectives. The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.
(3) Alternate Storage Site | Accessibility. The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

GSA Implementation Guidance: Control CP-6 and enhancements CP-6(1) and (3) are applicable at the FIPS 199 Moderate and High levels. Enhancement CP-6(2) is applicable at the FIPS 199 High level.

FIPS 199 Moderate and High impact systems must have an alternate storage site that is capable of protecting and restoring information system backup data in the event of a disruption at the primary location. In addition to this requirement, agreements must be made between the system owner/organization and the alternate storage provider in order to ensure storage and recovery capabilities are in place and that they meet the system's recovery objectives.

The following criteria must be used when considering alternate storage sites and vendors in accordance with NIST SP 800-34, Chapter 3.

- **Geographic area:** distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site;
- **Accessibility:** length of time necessary to retrieve the data from storage and the storage facility's operating hours;
- **Security:** security capabilities of the shipping method, storage facility, and personnel; all must meet the data's security requirements;
- **Environment:** structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls); and
- **Cost:** cost of shipping, operational fees, and disaster response/recovery services.

Develop and document a formal agreement such as an MOU or SLA addressing the requirements listed in NIST SP 800-34, Chapter 3.

For enhancements CP-6(1) and (3), FIPS 199 Moderate and High impact systems must have an alternate storage site identified in the system's contingency and security plans. The alternate

storage site and accessibility to it must have sufficient physical separation from the primary site to prevent the same hazards from affecting it that is affecting the primary site, as identified in the system's risk assessment.

For enhancement CP-6(2), FIPS 199 High impact systems must ensure any alternate storage site that has been selected is configured to ensure the system's recovery time objective is met during recovery operations.

Additional Contractor System Considerations: *None.*

4.6 CP-7 Alternate Processing Site

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*information system operations*] for essential missions/business functions within [*GSA S/SO or Contractor recommended time period approved by the GSA AO consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Control Enhancements:

(1) Alternate Processing Site | Separation from Primary Site. The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
(2) Alternate Processing Site | Accessibility. The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
(3) Alternate Processing Site | Priority of Service. The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).
(4) Alternate Processing Site | Preparation for Use. The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

GSA Implementation Guidance: Control CP-7 is not applicable at the FIPS 199 Low level. CP-7 and enhancements CP-7(1), (2), and (3) are applicable at the FIPS 199 Moderate and High levels. Enhancement CP-7(4) is applicable at the FIPS 199 High level.

FIPS 199 Moderate and High impact systems must have an alternate processing site containing the appropriate equipment and supplies to support the information system and is capable of resuming system operations within the allowable timeframe established by the BIA.

Alternate processing facilities are integral to contingency planning; they enable an information system to resume operation in the event of a system or area-wide disruption at the primary site. NIST SP 800-34, Chapter 3 defines three main alternate site types and examples of two variations of such sites as listed below.

- **Cold Sites** are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
- **Warm Sites** are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
- **Hot Sites** are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
- **Mirrored Sites** are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
- **Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

In order to ensure the alternate processing site can support the specific needs and requirements of the system, all FIPS 199 Moderate and High impact systems must develop and document a formal agreement such as an MOU or SLA. The MOU/SLA should address the following items.

- Contract/agreement duration;
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules;
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures);
- Site/facility priority access and/or use;
- Site availability;
- Site guarantee;
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable;
- Contract/agreement change or modification process;
- Contract/agreement termination conditions;
- Process to negotiate extension of service;
- Guarantee of compatibility;
- Information system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software);

- Change management and notification requirements, including hardware, software, and infrastructure;
- Security requirements, including special security needs;
- Staff support provided/not provided;
- Facility services provided/not provided (use of onsite office equipment, cafeteria, etc.);
- Testing, including scheduling, availability, test time duration, and additional testing, if required;
- Records management (onsite and offsite), including electronic media and hardcopy;
- Service-level management (performance measures and management of quality of information system services provided);
- Work space requirements (e.g., chairs, desks, telephones, personal computers);
- Supplies provided/not provided (e.g., office supplies);
- Additional costs not covered elsewhere;
- Other contractual issues, as applicable; and
- Other technical requirements, as applicable.

For enhancements CP-7(1), (2), and (3), FIPS 199 Moderate and High impact systems must select an alternate processing site that is physically separated from the primary site to ensure it is not susceptible to the same hazards as identified in the risk assessment. The alternate processing site must also be reviewed to verify the same level of security measures are applied as required by the systems FIPS 199 impact level, as well as to identify any site-specific problems that may need to be remediated in order to ensure successful recovery and operation of the information system.

For enhancement CP-7(4), FIPS 199 High impact systems must have an alternate processing facility that is configured to resume operations of the information system or its business/mission critical components.

Additional Contractor System Considerations: None.

4.7 CP-8 Telecommunications Services

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*information system operations*] for essential missions and business functions within [*GSA S/SO or Contractor recommended time period approved by the GSA AO*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Control Enhancements:

(1) Telecommunications Services | Priority of Service Provisions. The organization:
   (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) Telecommunications Services | Single Points of Failure. The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) Telecommunications Services | Separation of Primary / Alternate Providers. The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

(4) Telecommunications Services | Provider Contingency Plan. The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*at least annually*].

GSA Implementation Guidance: Control CP-8 is not applicable at the FIPS 199 Low level. Control CP-8 and enhancements CP-8(1) and (2) are applicable at the FIPS 199 Moderate and High levels. Enhancements CP-8(3) and (4) are applicable at the FIPS 199 High level.

FIPS 199 Moderate and High impact systems must ensure any system disruption caused by a loss of telecommunications is mitigated by an alternate telecommunications service. Similar to the implementation of alternate processing sites in the event of system failure, the establishment of alternate telecommunications services is equally important.

For enhancements CP-8(1) and (2), FIPS 199 Moderate and High impact systems must have priority of service provisions in place at the primary and alternate processing sites in order to ensure the availability requirements of the information system are met. In addition, if a common carrier is used for telecommunications services for national security emergency preparedness, there must be a service priority agreement in place.

For enhancements CP-8(3) and (4), FIPS 199 High impact systems must use an alternate telecommunications provider separate from the primary provider to ensure no single point of failure exists for the system. Alternate communications providers servicing FIPS 199 High impact systems must have contingency plans in place.

Additional Contractor System Considerations: *None.*

4.8 CP-9 Information System Backup

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*using at least a Grandfather-Father-Son scheme with daily incremental and weekly full*];

b. Conducts backups of system-level information contained in the information system [*using at least a Grandfather-Father-Son Scheme with daily incremental and weekly full*];
c. Conducts backups of information system documentation including security-related documentation [*using at least a Grandfather-Father-Son Scheme with daily incremental and weekly full*]; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Control Enhancements:

(1) Information System Backup | Testing for Reliability / Integrity. The organization tests backup information [*at least annually*] to verify media reliability and information integrity.
(2) Information System Backup | Test Restoration Using Sampling. The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.
(3) Information System Backup | Separate Storage for Critical Information. The organization stores backup copies of [*the information system's operating system(s), other critical software, and inventory*] in a separate facility or in a fire-rated container that is not collocated with the operational system.
(5) Information System Backup | Transfer to Alternate Storage Site. The organization transfers information system backup information to the alternate storage site [*GSA S/SO or Contractor recommended and AO approved time period and transfer rate in accordance with the recovery time and recovery point objectives*].

GSA Implementation Guidance: Control CP-9 is applicable at all FIPS 199 levels. Enhancement CP-9(1) is applicable at FIPS 199 Moderate and High levels. Enhancements CP-9(2), (3), and (5) are applicable at FIPS 199 High level.

All systems must ensure backups are performed on user and system level information and all relevant system documentation including security documentation. In addition, the backups must be secured at their storage location. NIST SP 800-34, Chapter 5 provides detailed guidance on selecting and implementing an effective backup strategy as well as implementing the appropriate data security in order to maintain the integrity of system data and software.

GSA policy requires a Grandfather-Father-Son backup scheme (GFS Scheme) with daily incremental and weekly full backups to be performed for each of the information types identified in the control objectives. The protection of backup data at the alternate storage location must be implemented in accordance with the NIST SP 800-53 requirements per FIPS 199 impact level. Typical protective mechanisms include the use of digital signatures and cryptographic hashes.

For enhancement CP-9(1), FIPS 199 Moderate and High impact systems must test their backup information at least annually.

For enhancements CP-9(2), (3), and (5) FIPS 199 High impact systems must use a sample of their backup information for restoration of selected system functions during contingency plan testing. Backup copies of the information systems inventory and critical software components such as applications and operating systems software, must be maintained separate from the primary operating facility or stored in fire-rated container(s).

Additional Contractor System Considerations: *None.*

4.9 CP-10 Information System Recovery and Reconstitution

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Control Enhancements:

(2) Information System Recovery and Reconstitution | Transaction Recovery. The information system implements transaction recovery for systems that are transaction-based.

(4) Information System Recovery and Reconstitution | Restore Within Time Period. The organization provides the capability to restore information system components within [*GSA S/SO or Contractor recommended and AO approved time periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

GSA Implementation Guidance: Control CP-10 is applicable at all FIPS 199 levels. Enhancement CP-10(2) is applicable at the FIPS 199 Moderate and High levels. Enhancement CP-10(4) is applicable at the FIPS 199 High level.

Recovered information systems must have all security related configuration settings required by FIPS 199 impact level and all security-critical patches reinstalled prior to resumption of system operations.

For enhancement CP-10(2) FIPS 199 Moderate and High impact systems, all transaction based systems, such as databases and transaction processing systems, must be recovered using applicable transaction recovery mechanisms and system specific compensating security controls provided if the system cannot be completely recovered to a known state at the alternate processing site.

For enhancement CP-10(4), FIPS 199 High impact systems must be capable of reimaging system components from a secure configuration controlled disk image of the information system, within the identified recovery time objective as documented within the BIA and contingency plan.

Additional Contractor System Considerations: *None.*

5 Contingency Planning and Supply Chain Risk Management

NIST SP 800-161, recommends Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) practices be used for FIPS 199 High systems. ICT SCRM processes increase the costs, both financial and time expended in supporting them, not just for GSA, but also for system integrators, suppliers, and service providers. ICT SCRM should be considered in the context of the system's missions, operational environments, and risks. Due to the increased costs involved in incorporating SCRM in the contingency planning process the System Owner, IST Division Director, ISSM, and ISSO must carefully consider these costs prior to incorporating system specific SCRM processes into contingency planning. Any questions with regard to including SCRM controls should be sent to ispcompliance@gsa.gov

NIST SP 800-161 states, *"ICT supply chain concerns of contingency planning include planning for alternative suppliers of system components, alternative suppliers of systems and services, denial of service attacks to the supply chain, and planning for alternate delivery routes for critical system components. Additionally, many techniques used for contingency planning, such as alternative processing sites, have their own ICT supply chains including their own specific ICT supply chain risks. Organizations should ensure that they understand and manage ICT supply chain risks and dependencies related to the contingency planning activities as necessary."*

The CP controls addressed in NIST SP 800-161, limited to those controls for FIPS 199 High systems, are provided in the following sections along with NIST SP 800-161 supplemental guidance on the controls and GSA's implementation guidance.

5.1 CP-1 Contingency Planning Policy and Procedures (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain concerns into the contingency planning policy. The policy should cover ICT information systems and the ICT supply chain infrastructure and address:

a. Unplanned component failure and subsequent replacement;
b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and
c. Product unavailability.

GSA Implementation Guidance: FIPS 199 High systems that have integrated SCRM into their contingency plans must address the following areas in those plans. In addition to the documents described, supply chain risks are often addressed by contract clauses stipulating how vendors must address supply chain risks.

- Component failure and replacement. Generally, these two actions are covered in a system's configuration management (CM) plan. The CM plan and contingency plan must include how supply chain concerns are addressed.

- Replacement of components due to system lifecycle activities such as improvements, maintenance, upgrades, and modernization. The CM and contingency plans must include how these typical lifecycle occurrences address supply chain concerns.
- Product unavailability. Unavailability of existing products similarly must be addressed and is similar to replacement of a product.

Additional Contractor System Considerations: *Contractor systems may defer to GSA policy and procedures as identified above or separately implement policy and procedures that facilitate the implementation of SCRM.*

5.2 CP-2 Contingency Plan (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Organizations should define and implement a contingency plan for the ICT supply chain infrastructure so that there is no loss of data or operations. Contingencies should be put in place for the ICT supply chain infrastructure (including processes) and information systems (especially critical components) to ensure protection against compromise and to provide appropriate failover.

Control enhancements:

(2) Contingency Plan | Capacity Planning.
NIST SP 800-161 Supplemental ICT SCRM Guidance: This enhancement helps availability of the ICT supply chain infrastructure or information system components.

(8) Contingency Plan | Identify Critical Assets.
NIST SP 800-161 Supplemental ICT SCRM Guidance: Ensure that critical assets (including hardware, software, and personnel) are identified to ensure that appropriate contingency planning requirements are defined and applied to ensure continuity of operation. A key step in this process is to complete a criticality analysis on components, functions, and processes to identify all critical assets.

GSA Implementation Guidance: FIPS 199 High systems that have implemented SCRM processes in their contingency plans must address capacity planning, failover, redundancy, and the ability to restore/recover critical assets, functions, and processes. These actions may be covered in service level agreements or other contractual stipulations when vendors and third parties are involved. When vendors or third parties are used, the GSA S/SO must verify that their vendors/third parties also have addressed these areas in their contingency plans.

Additional Contractor System Considerations: *None.*

5.3 CP-6 Alternate Storage Site (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: When managed by system integrators or external service providers, alternate storage sites are considered within an organization's ICT supply chain infrastructure. Organizations should apply appropriate ICT supply chain controls to those storage sites.

Control enhancements:

(1) Alternate Storage Site | Separation from Primary Site
NIST SP 800-161 Supplemental ICT SCRM Guidance: This enhancement helps resiliency of ICT supply chain infrastructure.

GSA Implementation Guidance: FIPS 199 High systems that have implemented SCRM processes in their contingency plans must ensure that any supply chain risk mitigation measures are included for alternate storage sites.

Additional Contractor System Considerations: *None.*

5.4 CP-7 Alternate Processing Site (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: When managed by system integrators or external service providers, alternate storage sites are considered within an organization's ICT supply chain infrastructure. Organizations should apply appropriate ICT supply chain controls to those processing sites.

GSA Implementation Guidance: FIPS 199 High systems that have implemented SCRM processes in their contingency plans must ensure that any supply chain risk mitigation measures are included for alternate processing sites.

Additional Contractor System Considerations: *None.*

5.5 CP-8 Telecommunications Services (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Organizations should consider alternate telecommunication service providers for their ICT supply chain infrastructure and to support critical information systems.

Control enhancements:

(3) Telecommunications Services | Separation of Primary/Alternate Providers
NIST SP 800-161 Supplemental ICT SCRM Guidance: Separation of primary and alternate providers supports ICT supply chain resilience.

(4) Telecommunications Services |Provider Contingency Plan
NIST SP 800-161 Supplemental ICT SCRM Guidance: For ICT SCRM, system integrator and external service provider contingency plans should provide separation in infrastructure, service, process, and personnel, where appropriate.

GSA Implementation Guidance: FIPS 199 High systems that have implemented SCRM processes in their contingency plans must ensure Telecommunications Services providers have separation per the main CP-8 control and each has addressed SCRM in their contingency plans.

Additional Contractor System Considerations: *None.*

6 Summary

GSA contractors and Federal employees should use this guide and the noted references to facilitate implementation of contingency planning requirements. Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO ISP Division at ispcompliance@gsa.gov.

Appendix A: Contingency Planning Templates

The templates identified below are available on the GSA IT Security Forms InSite page and can be used to develop contingency planning documents and processes.

- Business Impact Analysis Template
- Contingency Plan Template for Low Impact System
- Contingency Plan Template for Moderate Impact System
- Contingency Plan Template for High Impact System
- Contingency Plan Test Plan Template
- Contingency Plan Test Report Template
- Contingency Plan Logistics Checklist Template

Appendix B: Contingency Plan Sample Test Scenarios

Provided in the table below are examples of possible Contingency Plan test scenarios and potential expected outcomes.

Example Contingency Test Scenario	Example Expected Outcome
System X maintained at Vendor Y is declared inoperable. The system must be restored at the alternate (Hot Site) facility where a sufficient communication network exists to support the system. Full back-up tapes from System X completed the night before are maintained at an offsite location (vault). Restore operations at the Alternate Facility (Hot Site) where the system can successfully be run on the recreated system.	☐ Backup tapes can be recovered in a timely manner. ☐ System can be recovered successfully on an alternate platform from backup media. The alternate production site assumes all functions of the system. ☐ Telecommunications can be switched and reconfigured to the alternate production site. ☐ Vendor, agency, and recovery team are able to coordinate recovery actions between teams. ☐ The system is functional on the alternate equipment. ☐ Procedures for restoring to normal operations are effective. ☐ Notification procedures are effective.
System X experiences multiple component failures and is declared inoperable. Failure include: ☐ Power failure (as if, short circuit, malfunction, etc.) ☐ Hard drive/disk failure as a result of power surge/short circuit and/or malfunction The following controls are in place: ☐ System Contingency Plan procedures for recovery action are established ☐ Redundant/ back-up power supply exist and available to maintain system operations ☐ Back-up Systems data is available and current ☐ Applications can be re-established on the System without losing operational status	☐ System contacts, vendors, and recovery teams are able to coordinate recovery actions. ☐ Procedures to address system component failures are contained in the system contingency plan. ☐ Procedures for restoring to normal operations are effective. ☐ Notification procedures are effective. ☐ Redundant power supply is available and system works as intended. ☐ System back-up/mirror image is current and available. ☐ System is recovered in the scheduled time window specified in the contingency plan.
System X maintains two sites that are replicas of one another. Only one is the production system. The production site is brought down for routine maintenance. The remaining site must assume all functions of the system. Telecommunications to the alternate are switched and/or reconfigured.	☐ System recovery at the alternate site is successful. The alternate production site assumes all functions of the system. ☐ Coordination among recovery teams is effective. ☐ Procedures for migration to replicate site is effective. ☐ Notification procedures are effective. ☐ Telecommunications are switched to the alternate production site. ☐ Users continue to post transactions to the system. ☐ System application back-ups are routinely accomplished. ☐ System back-up/mirror image is current and available. ☐ Operational status of the system is maintained.